

REMARKS

In the Official Action mailed on **January 13, 2005** the Examiner reviewed claims 1-11, 13-29, 31-47, and 49-54. Claims 1, 4, 5, 8, 9, 13, 15, 16, 18, 19, 22, 23, 26, 27, 31, 33, 34, 36, 37, 40, 41, 44, 45, 49, 51, 52, and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bruce Schneier (*Applied Cryptography 2nd Edition*, Oct. 1995, John Wiley & Sons Pub. pages 43-57, hereinafter "Schneier") in view of Medvinski et al (*Public Key Utilizing Tickets for Application Servers*, hereinafter "Medvinski"). Claims 14, 17, 32, 35, 50, and 53 were rejected as being unpatentable over Schneier in view of Medvinski and Official Notice (hereinafter "ON"). Claims 2, 3, 6, 7, 10, 11, 20, 21, 24, 25, 28, 29, 38, 39, 42, 43, 46, and 47 were rejected as being unpatentable over Schneier in view of Medvinski and Sirbu et al (*Public Key Based Ticket Granting service in Kerberos*, hereinafter "Sirbu") and ON.

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 19, and 37 were rejected as being unpatentable over Schneier in view of Medvinski. Applicant respectfully points out that Schneier teaches the secret key "must be in place **before** the start of the protocol" (see Schneier, page 47, chapter 3.1, first paragraph).

In contrast, the present invention uses a **temporary** secret, which is exchanged within the protocol and which becomes invalid after a specified time (see page 9, lines 23-26 of the instant application). This is beneficial because it allows a server to establish secure communications with a client without the need to have a secret key in place on the KDC before the start of the protocol. There is nothing within Schneier or Medvinski, either separately or in concert, which suggests using a temporary secret, which is exchanged as part of the protocol and which becomes invalid after a specified time.

Accordingly, Applicant has amended independent claims 1, 19, and 37 to clarify that the present uses a temporary secret, which is exchanged within the

protocol and which becomes invalid after a specified time. These amendments find support on page 9, lines 23-26 of the instant application.

Hence, Applicant respectfully submits that independent claims 1, 19, and 37 as presently amended are in condition for allowance. Applicant also submits that claims 2-11 and 13-18, which depend upon claim 1, claims 21-29 and 31-36, which depend upon claim 19, and claims 38-47 and 49-54, which depend upon claim 37, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By



Edward J. Grundler
Registration No. 47, 615

Date: March 16, 2005

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616
Tel: (530) 759-1663
FAX: (530) 759-1665